

Express Mailing Label No. EL600640932US

PATENT APPLICATION
Docket No. 15267.3

UNITED STATES PATENT APPLICATION

of

Travis Kelly Harper

and

Benjamin Clark Stout

for

**METHODS FOR ENCRYPTING AND DECRYPTING ELECTRONICALLY
STORED MEDICAL RECORDS AND OTHER DIGITAL DOCUMENTS FOR
SECURE STORAGE, RETRIEVAL AND SHARING OF SUCH DOCUMENTS**

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE

FO4TFO 02049260

BACKGROUND OF THE INVENTION

1. The Field of the Invention

The present invention is in the field of encryption and decryption of electronic documents, such as image or text documents in digital form, so as to provide enhanced security during storage, retrieval, sharing, and viewing of such documents. More particularly, the invention is in the field of encryption, decryption, and display of electronic records, such as digitized medical records that include sensitive information, so as to limit access to, and the ability to alter, such records, thereby preserving sensitive information contained therein.

2. Background and Related Art

Medical records are typically created, stored, transferred and copied in tangible form, typically as paper documents. Doctors most often create medical records by hand writing information onto pre-printed forms, which are manually placed within patient files. Such records may include times and dates of diagnosis and treatment of a patient, the condition being attended to, the symptoms that led to the diagnosis, and the specific procedures, medicine or other care used in treatment of the condition. The records may also include other personal and confidential information, some or all of which may be protected by the patient-doctor privilege.

The patient-doctor privilege exists, among other things, to encourage full disclosure of medical conditions and other matters of a potentially personal nature, both past and present, between doctor and patient. Full disclosure facilitates diagnosis and treatment. Confidence that information disclosed will be kept confidential promotes open and honest communication and disclosure between doctor and patient. Conversely, fear

1 that confidential and sensitive information between a doctor and patient might be
2 disclosed to others may inhibit full disclosure, thus compromising the ability of a doctor
3 to adequately treat a patient. To allay such fears, the law strictly regulates who can
4 access sensitive patient records.

5 In view of the patient-doctor privilege, and pursuant to standard professional
6 custom, hospitals, clinics, doctor's offices and other facilities that store confidential
7 medical records usually have procedures and safeguards for maintaining the
8 confidentiality of records. Where such records are kept in tangible form, restricting
9 access through security clearance measures is straightforward. When copies of records
10 are created, controlling access becomes more difficult. Where records are copied in
11 tangible form, it is a matter of limiting and controlling access to the tangible copy,
12 typically through strict contractual provisions as well as the aforementioned legal
13 restrictions on who rightfully has access to a confidential medical record. Where the
14 medical record is copied into digital form, special measures must be followed to prevent
15 unauthorized access, copying, and distribution. Moreover, because digital documents are
16 generally more easily altered or obliterated, safeguards must ensure the integrity of the
17 medical record from unauthorized alteration or obliteration.

18 Examples of security systems for limiting access to sensitive medical records
19 and/or preventing unauthorized alteration thereof are set forth in U.S. Patent No.
20 5,619,571 to Sandstrom et al., U.S. Patent No. 5,784,461 to Shaffer et al., U.S. Patent No.
21 5,579,393 to Conner et al., and U.S. Patent No. 5,809,145 to Slik et al. The foregoing
22 patents mainly disclose encrypted passwords and fragments of the document in question
23 to prevent access to the actual document. They do not generally involve encrypting an
24 entire file and then making the encrypted file publicly available, though unintelligible,

1 such as when an electronic document is sent in encrypted form through the Internet.

2 Whereas the foregoing patents may provide adequate security *vis-à-vis* closed computer
3 systems or networks where access is generally limited, they may not adequately protect
4 the confidentiality and integrity of digital documents that are publicly accessible or
5 shared in a manner that does not prevent unauthorized third parties from capturing such
6 digital documents.

7 A common encryption method used currently with regard to Internet transactions
8 is the Rivest-Shamir-Aldeman (RSA) encryption algorithm (U.S. Patent No. 4,405,829
9 to Rivest et al.), which relies on a public key (or asymmetric) protocol. RSA encryption
10 uses extremely large prime numbers that require an exponential amount of time to
11 decipher, where the exponent is determined by the size of the number of bits that make
12 up the prime number. In RSA encryption, the public key may be used by anyone to
13 encrypt an original electronic document ("plaintext" or "cleartext") but cannot be used to
14 decrypt (or decipher) the encrypted document ("ciphertext"). Only someone having
15 access to the private key can decrypt or decipher the encrypted file.

16 RSA encryption is therefore well suited for systems in which a large number of
17 parties (e.g., clients) wish to send encrypted data to one central party (e.g., a financial
18 institution). The public key can be made generally available to the public at large, such
19 as through web browser implemented encryption when the client logs into the central
20 party's web site. This allows every client to encrypt sensitive information before sending
21 it to the central party using the same public key. Because only the central party has
22 possession or access to the private key, only the central party can decrypt the encrypted
23 data that is sent to it over the Internet. Presently, 128-bit RSA encryption is the standard
24 protocol for sending sensitive information from a client to a centralized institution such

1 as a bank, online broker, or other financial institution. This Internet protocol is
2 commonly referred to as HyperText Transfer Protocol Secure (HTTPS), and the
3 encryption is commonly referred to as Secure Socket Layer (SSL).

4 Nevertheless, because it is necessary to restrict access to the private key to
5 prevent unauthorized capture and access of encrypted data, asymmetric encryption
6 methods such as RSA encryption may not be best suited in the case where a central party
7 wishes to send one or more encrypted files to a number of different receiving parties who
8 will need to decrypt the encrypted files. In such cases, the private key will have to be
9 made available to all such receiving parties. As is plainly seen, making the private key
10 generally available to a number of different parties obviously reduces the ability of the
11 central party to keep the private key secret, thus comprising the privacy of the
12 information being sent to the different parties over the Internet or other nonsecure
13 channel.

14 Another problem with conventional encryption and decryption methods and
15 systems, whether symmetric or asymmetric encryption, is that once the receiving party
16 has been given the ability to decrypt the encrypted message so as to recover the original
17 plaintext file, there is nothing to prevent that party from saving, altering, or sending the
18 decrypted plaintext file to an unauthorized party.

19 In view of the foregoing, it would be an improvement in the art to provide
20 encryption and decryption methods and systems that were specifically tailored for use by
21 a central party who wishes to securely send encrypted files to a number of different
22 receiving parties while maintaining control over the key(s) necessary to decrypt the
23 encrypted files.

1 In particular, improved encryption and decryption methods and systems are
2 needed that could adequately prevent unauthorized access to medical records or other
3 confidential electronic documents transmitted over nonsecure communications channels,
4 such as the Internet, by a central party to a number of different receiving parties.

5 It would be an additional improvement in the art to provide improved encryption
6 and decryption methods and systems that were integrated with a display system that
7 allowed the receiving party to view the decrypted plaintext document but which could, if
8 desired, be configured to prevent the viewing party from saving, altering or sending the
9 decrypted plaintext file to an unauthorized party.

10 Such methods and systems for encrypting, decrypting and displaying sensitive
11 medical records and other electronic documents or files are disclosed and claimed herein.
12
13
14
15
16
17
18
19
20
21
22
23
24

SUMMARY OF THE INVENTION

The present invention relates to methods and systems for encrypting and decrypting electronic graphic or other files. The encryption and decryption algorithms may advantageously be integrated within specialized viewing software that could be configured, if desired, to prevent the viewing party from saving, altering or sending the decrypted plaintext file to an unauthorized party. The inventive methods and systems are particularly suitable when third-party access to the actual electronic file cannot be prevented, such as when an encrypted file is transmitted over the Internet or other public or quasi-public communications channel.

The methods and systems of the invention for securely encrypting and then decrypting files are suitable for use with graphic files, such as an electronic document that is a "Tagged Image Format File" (TIFF or .tif). Of course, the inventive methods and systems could be used to encrypt and decrypt other types of files, such as text files or JPEG, BMP, GIF files, and the like. An example of a present use for the inventive encryption methods and systems is where a custodian of sensitive and confidential medical records wishes to share such records over a nonsecure communications channel, such as the Internet, with a number of authorized third parties, such as life insurers, property and casualty insurers, and personal-injury and defense attorneys. Of course, the inventive encryption methods and systems may be used to protect the security of virtually any sensitive or confidential electronic document, whether in graphic or text form.

The inventive encryption methods and systems utilize an essentially symmetric encryption and decryption algorithm in which a single set of keys is used in both the encryption and decryption processes. A point of departure from conventional symmetric encryption systems is that the key used to first encrypt the plaintext and then decrypt the

1 ciphertext (the “encryption key”) is divided into two or more distinct subcomponents.
2 One component of the encryption key (referred to herein as the “public key”) is provided
3 along with the encrypted ciphertext. A second component of the encryption key (referred
4 to herein as the “private key”) is known only to the encrypting party and to the one or
5 more parties authorized to decrypt the ciphertext. A mathematical algorithm used to
6 meaningfully integrate and utilize the information contained in the public and private
7 components of the encryption key is also preferably known only to the encrypting party
8 and the authorized decrypting parties. Depending on the level of security that is desired,
9 such as when viewed in the context of who the parties to the transaction are, what the
10 value of the information contained in the encrypted documents is (presently and over
11 time), and how much time and effort must be expended to either decipher the encryption
12 key, the ciphertext, or both, alternate procedures having varying levels of safety and
13 security may be utilized in, or to grant or restrict access to, the private component of the
14 encryption key.

15 The “public key” is essentially an array of random numbers and the “private key”
16 is a block of random data. The random numbers in both the public and private keys may
17 be generated using random number generation means known in the art. Depending on
18 the level of security and randomness that is desired, either or both of the public and
19 private keys may be generated for each electronic file to be encrypted or else used to
20 encrypt more than one file. Generating new public and/or private keys for each
21 electronic file greatly increases the difficulty of a hacker in deciphering the code and
22 accessing the encrypted files. Generating a new private key for each encrypted electronic
23 file is, in some ways, at least partially akin to a “one-time pad” encryption system, which
24 is theoretically the most secure encryption system possible.

1 To restrict availability to unauthorized parties, the private key and encryption
2 algorithm may be embedded or hard-coded within the computer-executable instructions
3 or software used to decrypt and view the decrypted file. Alternatively, the decrypting
4 party may be required to obtain the private key and at least a portion of the encryption
5 algorithm at the time of decryption, such as by means of a password-protected login
6 procedure over a secure channel. The latter would more securely protect the security and
7 integrity of the file in the event that an unauthorized third party were to intercept the
8 encrypted file and public key, and were to somehow secure a copy of the viewing
9 software.

10 In an exemplary encryption process within the scope of the invention, the original
11 data stream, or "cleartext," is encrypted one byte (eight bits) at a time by performing an
12 "exclusive-or" (XOR) process for each byte against one or more random number values
13 taken from the public key. The private key, by means of a mathematical algorithm, is
14 used to select one or more random numbers from the public key each time a byte of the
15 data stream is encrypted. The encrypted bytes are stored as the encrypted data. In an
16 exemplary method for storing and sending the encrypted file, the public key is stored
17 with the encrypted data stream to yield a unique file type that is decrypted and displayed
18 using special software provided by the encrypting party.

19 Without limiting the general nature of the invention, the inventive encryption
20 processes are especially well suited in the case where a single encrypting party wishes to
21 securely send encrypted files to a number of different receiving parties. An example is
22 where a central repository of medical records, which are typically hand-written then
23 converted and saved in graphic form (e.g., as a TIFF file), wishes to securely send a
24

1 medical record to one or more receiving requesting parties who are authorized to view the
2 medical record in question over a nonsecure channel, such as the Internet.

3 In an exemplary decryption process, the ciphertext is decrypted using the same
4 public and private keys used to encrypt the plaintext. So long as the same mathematical
5 algorithm is used for decryption that was used for encryption, and because the XOR
6 process is reversible, the encrypted data may be decrypted (*e.g.*, one byte at a time) by
7 means of the same random number values from the public table using the same XOR
8 process to yield the original cleartext.

9 In the case where the ciphertext is an encrypted graphic file, the decryption
10 algorithm may advantageously be integrated within a specialized viewing program that
11 integrates decryption and display of the graphic file. In a preferred method for ensuring
12 the security and integrity of the original document, the viewer (*e.g.*, a TIFF viewer)
13 supplied to the decrypting party will prevent, or at least make it extremely difficult and
14 illegal, for the viewing party to alter the decrypted image file in any way, and/or save the
15 decrypted cleartext file, and/or encrypt cleartext files, and/or display any file that is not
16 an encrypted TIFF file stored together with the public key. Such alterations will at least
17 make it difficult to pass off an altered file as the originally sent file. Additional features
18 of the preferred viewing program will be discussed more fully below.

19 Accordingly, it is an object of the invention to provide improved encryption and
20 decryption methods and systems specifically tailored to prevent unauthorized capture or
21 access to a sensitive medical record transmitted over a public or quasi-public
22 communications channel, such as the Internet.

23 It is a further object to provide encryption and decryption methods and systems
24 which not only prevent unauthorized capture or access to sensitive records sent via the

1 Internet or other public channel but which prevent unauthorized alteration of the record in
2 the event that unauthorized access was achieved.

3 It is an additional object to provide methods and systems for the encryption of
4 files and subsequent decryption and display which not only prevent unauthorized access
5 or alteration of an electronic document but which also indicate to the custodian of the
6 record if someone had, in fact, altered, or attempted to alter, the electronic document.

7 Additional features and advantages of the invention will be set forth in the
8 description which follows, and in part will be obvious from the description, or may be
9 learned by the practice of the invention. The features and advantages of the invention
10 may be realized and obtained by means of the instruments and combinations particularly
11 pointed out in the appended claims. These and other features of the present invention
12 will become more fully apparent from the following description and appended claims, or
13 may be learned by the practice of the invention as set forth hereinafter.

14
15
16
17
18
19
20
21
22
23
24

BRIEF DESCRIPTION OF THE DRAWINGS

To describe the manner in which the above-recited and other advantages and features of the invention can be obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2A is a schematic diagram illustrating an exemplary encryption system according to the invention;

Figure 2B is a schematic diagram illustrating an exemplary decryption system according to the invention;

Figure 3 is a schematic diagram illustrating an exemplary communication system between an encrypting party and a decrypting party;

Figure 4 is a schematic diagram illustrating an exemplary system for decrypting and outputting the original electronic file according to the invention;

Figure 5A is a flow diagram depicting an exemplary process by which an original electronic file is encrypted and then stored as a unique file type according to the invention;

Figure 5B is a flow diagram depicting an exemplary process by which an encrypted file is decrypted according to the invention;

1 Figure 6 illustrates a detailed process according to the invention by which a block
2 of the cleartext is encrypted and/or a block of ciphertext is decrypted; and

3 Figure 7 illustrates an exemplary algorithm for serially selecting random numbers
4 from the private key during encryption of each block of cleartext or decryption of each
5 block of ciphertext according to the invention.

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

Although the term “encryption algorithm” may normally refer to the specific mathematical algorithm used in the actual encryption and/or decryption processes, for simplicity and brevity this term shall also include, as a subcomponent, the mathematical algorithm used to meaningfully utilize and integrate the public and private components of

1 the encryption keys used according to the invention. The latter algorithm may more
2 specifically be referred to as the "encryption key algorithm," or simply "the key
3 algorithm."

4 Although the term "public key" is typically used in the art to refer to a publicly
5 available encryption key that is given to clients of a central institution for the purpose of
6 encrypting and sending private information from a client to the institution, but which
7 cannot be used to decrypt the encrypted file (*i.e.*, in asymmetric encryption), for purposes
8 of this disclosure and the appended claims, the term "public key" shall refer to the
9 subcomponent of the encryption key that is sent together with the encrypted file from the
10 sender to the receiver of an encrypted file. Thus, the "public key" is not really "public"
11 in the conventional sense but is so described because it is packaged and sent together
12 with the encrypted file, typically over the Internet, such as via a secure HTTPS channel.
13 Moreover, the "public key" is used for both encryption and decryption of electronic files
14 (*i.e.*, in symmetric encryption).

15 Although the term "private key" is typically used in the art to refer to the
16 decryption key that is only known to the deciphering party in asymmetric encryption, for
17 purposes of this disclosure and appended claims, the term "private key" shall refer to the
18 subcomponent of the encryption key that is not sent with the encrypted file but which is
19 known only to the sender and the receiver of the encrypted file. Thus, access to the
20 "private key" is limited to the encrypting and decrypting parties. Like the public key, the
21 "private key" is also used for both encryption and decryption of electronic files in a
22 symmetric encryption system.

23 The terms "cipher" or "key" generally relate to both the public key and the private
24 key, but especially refer to the interaction between the public and private keys to yield a

1 single symmetrical cipher or key system used in both encrypting and decrypting
2 electronic files.

3 The terms “exclusive or” or “XOR” refer to the process by which a first binary
4 number is compared to a second binary number so as to yield a third binary number. For
5 purposes of this disclosure and the appended claims, it shall be understood that the binary
6 equivalent of an integer value is used in the XOR process because this process is unique
7 to binary numbers. Thus, when a block of binary data is “XORed” with an integer value
8 selected from an encryption key, it is to be understood that it is the binary equivalent of
9 the integer value that is really being used in the XOR process.

10 The term “encrypting party” shall mean the actual person or entity that encrypts a
11 particular plaintext file so as to generate a corresponding ciphertext file, together with
12 any affiliates, agents or representatives. Similarly, the term “decrypting party” shall
13 mean the actual person or entity that decrypts a particular ciphertext file so as to restore
14 the corresponding plaintext file, together with any affiliates, agents or representatives.

15
16 **II. SYSTEMS FOR REQUESTING AND PROVIDING DIGITAL COPIES OF**
17 **MEDICAL DOCUMENTS.**

18 **A. Basic Operating System.**

19 The present invention extends to both methods and systems for encrypting and
20 decrypting electronic files, as well as sending and outputting such files. The
21 embodiments of the present invention may comprise a special or general purpose
22 computer including various computer hardware, as discussed in greater detail below.

23 Embodiments within the scope of the present invention also include computer-
24 readable media for carrying or having computer-executable instructions or data structures

1 stored thereon. Such computer-readable media can be any available media that can be
2 accessed by a general purpose or special purpose computer. By way of example, and not
3 limitation, such computer-readable media may include random access memory (RAM),
4 read only memory (ROM), electrically erasable programmable read only memory
5 (EEPROM), compact disc read only memory (CD-ROM), digital video disc (DVD), or
6 other optical disk storage, magnetic disk storage or other magnetic storage devices, or
7 any other medium which can be used to carry or store desired program codes in the form
8 of computer-executable instructions or data structures and which can be accessed by a
9 general purpose or special purpose computer. When information is transferred or
10 provided over a network or another communications connection (either hardwired,
11 wireless, or a combination of hardwired or wireless) to a computer, the computer
12 properly views the connection as a computer-readable medium. Thus, any such
13 connection is properly termed a computer-readable medium, as would be any medium for
14 transmitting a propagated signal. Combinations of the above should also be included
15 within the scope of computer-readable media. In addition to computer-readable media,
16 computer-executable instructions or data structures may be partly or wholly provided to
17 or sent from a computer in the form of a propagated wave, typically by means of one or
18 more communications connections between two or more computers. Computer-
19 executable instructions comprise, for example, instructions and data which cause a
20 general purpose computer, special purpose computer, or special purpose processing
21 device to perform a certain function or group of functions.

22 Figure 1 and the following discussion are intended to provide a brief, general
23 description of a suitable computing environment in which the invention may be
24 implemented. Although not required, the invention will be described in the general

1 context of computer-executable instructions, such as program modules, being executed
2 by computers in network environments. Generally, program modules include routines,
3 programs, objects, components, data structures, etc., that perform particular tasks or
4 implement particular abstract data types. Computer-executable instructions, associated
5 data structures, and program modules represent examples of the program-code means for
6 executing steps of the methods disclosed herein. The particular sequences of such
7 executable instructions or associated data structures represent examples of corresponding
8 acts for implementing the functions described in such steps.

9 Those skilled in the art will appreciate that the invention may be practiced in
10 network computing environments with many types of computer system configurations,
11 including personal computers (PCs), hand-held devices, multi-processor systems,
12 microprocessor-based or programmable consumer electronics, networked PCs,
13 minicomputers, mainframe computers, and the like. The invention may also be practiced
14 in distributed computing environments where tasks are performed by local and remote
15 processing devices that are linked (either by hardwired links, wireless links, or by a
16 combination of hardwired or wireless links) through a communications network. In a
17 distributed computing environment, program modules may be located in both local and
18 remote memory storage devices.

19 With reference to Figure 1, an exemplary system for implementing the invention
20 includes a general purpose computing device in the form of a conventional computer
21 system 10, which, in its broadest sense, includes components hardwired or otherwise
22 associated together within a conventional computer box, bundle, or subsystem illustrated
23 by item number 12, together with user interface, communications, and other devices and
24 features located externally to, physically separated from, or otherwise spaced apart

1 relative to the computer bundle or subsystem 12. By way of example, and not limitation,
2 a conventional computer bundle or subsystem 12 includes a processing unit 14, a system
3 memory 16, and a system bus 18 that couples various system components including the
4 system memory 16 to the processing unit 14. The system bus 18 may be any of several
5 types of bus structures including a memory bus or memory controller, a peripheral bus,
6 and a local bus using any of a variety of bus architectures. The system memory includes
7 read only memory (ROM) 20 and random access memory (RAM) 22. A basic
8 input/output system (BIOS) 24, containing the basic routines that help transfer
9 information between elements within the computer system 10, such as during start-up,
10 may be stored in ROM 20.

11 The computer system 10, typically the computer bundle or subsystem 12, may
12 also include a magnetic hard disk drive 26 for reading from and writing to a magnetic
13 hard disk 28, a magnetic disk drive 30 for reading from or writing to a removable
14 magnetic storage device 32, and an optical disk drive 34 for reading from or writing to a
15 removable optical disk 36 such as a CD-ROM, digital versatile disk, a laser disk, or other
16 optical media. The magnetic hard disk drive 26, magnetic disk drive 30, and optical disk
17 drive 34 are connected to the system bus 18 by a hard disk drive interface 38, a magnetic
18 disk drive-interface 40, and an optical drive interface 42, respectively. The drives and
19 their associated computer-readable media provide nonvolatile storage of computer-
20 executable instructions, data structures, program modules, and other data for the
21 computer 10. Although the exemplary environment described herein employs a magnetic
22 hard disk 28, a removable magnetic disk 32, and a removable optical disk 36, other types
23 of computer readable media for storing data can be used, including magnetic cassettes,
24 flash memory cards, Bernoulli cartridges, RAMs, ROMs, and the like. For purposes of

1 the specification and the appended claims, the term "computer readable medium" may
2 either include one or a plurality of computer readable media, working alone or
3 independently, so long as they singly or collectively form part of a recognizable system
4 for carrying out the processes of the invention.

5 Program code comprising one or more program modules may be stored on the
6 hard disk 28, magnetic disk 32, optical disk 36, ROM 20, or RAM 22, including an
7 operating system 44, one or more application programs 46, other program modules 48,
8 and program data 50. A user may enter commands and information into the computer
9 bundle or subsystem 12 by means of a keyboard 52, a pointing device (*e.g.*, "mouse") 54,
10 or other input devices (not shown), such as a microphone, joy stick, game pad, satellite
11 dish, scanner, video player, camera, or the like. These and other input devices are often
12 connected to the processing unit 14 through a serial port interface 56 coupled to the
13 system bus 18. Alternatively, these and other devices 58 may be connected by other
14 interfaces 60, such as a parallel port, a sound adaptor, a decoder, a game port or a
15 universal serial bus (USB). Nonexhaustive examples of "other devices 58" include
16 scanners, bar code readers, external volatile and nonvolatile memory or storage devices,
17 audio devices, video devices, and microphones. A monitor 62 or another display device
18 is also connected to the system bus 18 via an interface, such as a video adapter 64. In
19 addition to the monitor 62, computers typically include other output devices (generally
20 depicted as "other devices 58"), such as speakers and printers.

21 The computer system 10 may operate in or involve a networked environment
22 using logical connections to one or more remote computers, such as remote computers
23 64a and 64b. Remote computers 64a and 64b may each be another personal computer, a
24 server, a router, a network PC, a peer device or other common network node, and

1 typically include many or all of the elements described above relative to the computer
2 system 10, although only memory storage devices 66a and 66b and their associated
3 application programs 68a and 68b have been illustrated in Figure 1. The logical
4 connections depicted in Figure 1 include a local area network (LAN) 70 and a wide area
5 network (WAN) 72 that are presented here by way of example and not limitation. Such
6 networking environments are commonplace in office-wide or enterprise-wide computer
7 networks, intranets, and the global computer network or "Internet".

8 When used in a LAN networking environment, the computer bundle or subsystem
9 12 is connected to the local network 70 through a network interface or adapter 74. When
10 used in a WAN networking environment, the computer bundle or subsystem 12 may
11 include a modem 76, a wireless link, or other means for establishing communications
12 over the wide area network 72, such as the Internet. The modem 76, which may be
13 internal or external, is typically connected to the system bus 18 via the serial port
14 interface 56. In a networked environment, program modules depicted relative to the
15 computer bundle or subsystem 12, or portions thereof, may be stored in a remote memory
16 storage device (e.g., remote storage devices 66a and 66b). It will be appreciated that the
17 network connections shown are exemplary, and other means of establishing
18 communications over wide area network 72 may be used.

19 Although computer components are commonly arranged in the form depicted in
20 Figure 1, with some components of the computer system 10 physically located within,
21 and other components physically located outside, the computer bundle or subsystem 12, it
22 will readily be appreciated that the terms "computer" and "computer system" should be
23 broadly understood to include any or all of the foregoing components in any desired
24 configuration which facilitate carrying out the inventive methods and systems disclosed

herein. The terms “computer” and “computer system” may therefore include other common features or components not depicted in Figure 1.

B. Encryption and Decryption Systems.

Exemplary encryption and decryption systems within the scope of the invention are depicted more particularly in Figures 2A and 2B. Figure 2A illustrates an inventive encryption system 90 that may be used to encrypt an original plaintext file and then store the ciphertext together with the public key to yield a new file type. The encryption system 90 essentially includes an original electronic file 100, comprising plaintext blocks 102 (*e.g.*, A–E *etc.*) to be encrypted, and an encryption module 106, comprising an encryption algorithm 108, a private key 110 and a public key 112. Operation of the encryption system 90 yields a new file type 116, comprising encrypted ciphertext 118 and the public key 112, which, although depicted in Figure 2A, do not strictly constitute part of the encryption system 90. The ciphertext 118 further comprises encrypted blocks 120 (*e.g.*, A’–E’ *etc.*), which at least partially correspond to plaintext blocks 102 (*e.g.*, A–E *etc.*).

In a preferred embodiment, the original electronic file 100 will be encrypted one block at a time. Figure 2A therefore depicts a stream 104 of original plaintext blocks 102 being input from the original electronic file 100 to the encryption module 106. Also depicted is a stream 114 of encrypted blocks 120 being generated by the encryption module 106, as well as the public key 112, which are stored together as part of the new file type 116. The system depicted in Figure 2A may be embodied by any computing means known in the art, including those depicted in Figure 1 and described above.

1 The size of the plaintext blocks 102 to be encrypted can vary according to the
2 desired difficulty level in breaking the cipher. In general, the larger the blocks, the more
3 difficult it is to break the cipher. On the other hand, the size of the encryption key will
4 correspond to the size of the blocks. Thus, the length of the plaintext blocks 102 can be
5 selected to balance the desired level of security (*i.e.*, difficulty in breaking the cipher)
6 against concerns of reducing the storage space, memory and time required to encrypt and
7 decrypt a given file. In an exemplary system according to the invention, the plaintext
8 blocks 102 will comprise one byte (8 bits) of binary data, as will the encrypted blocks
9 120 and the random number values contained within the public key 112. Nevertheless, it
10 will be readily appreciated that the inventive systems may be generalized so as to be used
11 in encrypting plaintext blocks of any desired size.

12 The encryption module 106 preferably encrypts the original electronic file 100 to
13 yield the encrypted file 118 by means of the encryption algorithm 108 utilizing numeric
14 information supplied to it by the interaction of the private key 110 and public key 112.
15 Without limiting the general nature of the invention, in an exemplary embodiment within
16 the scope of the invention, the public key 112 provides one or more random numeric
17 values used to encrypt each plaintext block 102 using, *e.g.*, an “exclusive or” (XOR)
18 process, while the private key 110 provides random numeric values used to select, or
19 index, the one or more random values from the public key 112. In other words, while the
20 public key 112 provides the encryption algorithm 108 with the actual random value(s) to
21 XOR with each plaintext block 102 during encryption, the private key 110, according to a
22 special key algorithm embedded within the encryption algorithm 108, tells the encryption
23 algorithm 108 which random value(s) is/are to be selected from the public key 112 during
24 each encryption cycle.

1 The total number of random number values within the private and public keys 110
2 and 112 will depend on the level of security that is desired. In general, the greater the
3 number of random values the greater will be the task of breaking the cipher. On the other
4 hand, increasing the total number of random number values of the public key will
5 increase the size of the resulting encrypted file and may increase the time it takes to
6 encrypt and decrypt an electronic file. In general, in the case where blocks of binary
7 numbers are being serially decrypted, it will be preferable for the total number of random
8 numbers to be a power of 2 (*e.g.*, 256, 1024, 2048 or 16,384), according to common
9 convention. In an exemplary system according to the invention, the private key 110 and
10 the public key 112 will each contain a total of 2048 different random number values,
11 serially indexed from 0 to 2047 and randomly selected from possible numbers within a
12 predetermined range.

13 One weakness in any encryption system is where the key is far shorter (*i.e.*,
14 includes far fewer numbers) than the number of blocks to be encrypted, thus resulting in
15 repetition of the key sequences during encryption. This opens the door to hackers
16 identifying a pattern in the key, thus leaving a way to break the cipher and obtain the
17 information that has been encrypted using the deciphered key. In the present case, even
18 though the total number of random number values within the two keys is typically far less
19 than the number of blocks that are to be encrypted, repetition of the overall key (public
20 plus private portions) is highly unlikely due to the way in which the two keys are
21 mathematically related, as will be discussed more fully below. Even though a hacker
22 may have the public key in plain view, the failure to identify a sequence in the key as a
23 whole will make it very difficult to decipher the private portion of the key.

1 The ranges of possible random number values within the private key 110 and
2 public key 112 are determined by different criteria. The range of possible random
3 numbers within the private key 110 will generally be determined by the starting and
4 finishing index numbers of the public key 112. Thus, in the case where the public key
5 112 contains 2048 random numbers, serially indexed from 0 to 2047, the range of
6 possible random numbers within the private key 110 will include integers from 0 to 2047.

7 On the other hand, the range of possible random numbers within the public key
8 110 will generally be dependent on the size of the plaintext blocks 102 being encrypted.
9 In the case where the plaintext blocks 102 are one byte in length, the upper range of
10 possible random numbers within the public key 112 will be 255, which is the largest
11 possible integer having 1 byte of binary data (*i.e.*, $255 = 11111111$ in binary code).
12 Because the number 0 (00000000 in binary code) will return the original number in an
13 XOR process, it may be advantageous to limit the range of possible public key values to
14 non-zero integers so as to ensure a numeric change during each XOR process. Thus, in
15 the case where the plaintext is to be encrypted one byte at a time, the range of possible
16 random numbers within the public key 112 will preferably include integers from 1 to 255.
17 Of course, randomly returning the same number for a block of plaintext from time to time
18 will still yield an encrypted file that is difficult to decipher because the vast majority of
19 surrounding blocks of ciphertext will have been altered from the original plaintext.
20 Hence, the set of random numbers within the public key will be randomly or otherwise
21 selected from a set bounded below by 0 or 1 and bounded above by 255, or the largest
22 integer value corresponding to the binary blocks being encrypted/decrypted.

23 Reference is now made to Figure 2B, which illustrates an exemplary decryption
24 system 92 according to the invention that may be used to decrypt the new encrypted file

1 type 116 generated using the encryption system 90 of Figure 2A. The decryption system
2 92 essentially includes the new file type 116, comprising the public key 112 and
3 encrypted blocks 120 of ciphertext 118 to be decrypted, and a decryption module 106',
4 comprising a decryption algorithm 108' and the private key 110 and public key 112
5 utilized in the encryption module 106 described above with respect to the encryption
6 system 90. Operation of the decryption system 92 restores the original plaintext file 100,
7 which, although depicted in Figure 2B, does not strictly constitute part of the decryption
8 system 90. The decryption algorithm 108' is similar to the encryption algorithm 108,
9 except that the encryption algorithm 108 ultimately stores the public key 112 together
10 with the encrypted ciphertext file 118, while the decryption algorithm 108' discerns and
11 distinguishes the public key 112 from the encrypted ciphertext 120.

12 As in encryption, the encrypted file 118 is preferably decrypted one block at a
13 time. Figure 2B therefore depicts a stream 114' of encrypted blocks 120 (e.g., A'-E' etc.)
14 being input from the encrypted file 118 to the decryption module 106'. The new file type
15 116 provides the public key 112 to the decryption module 106'. Also depicted is a stream
16 104' of plaintext blocks 102 (e.g., A-E etc.) being generated by the decryption module
17 106', which together yield the original plaintext electronic file 100. The system depicted
18 in Figure 2B may be embodied by any computing means known in the art, including
19 those depicted in Figure 1 and described above.

20 As plainly seen by comparing the encryption and decryption systems depicted in
21 Figures 2A and 2B, respectively, the two systems are virtual mirror images of each other,
22 thus reflecting the fact that the encryption and decryption systems of the present
23 invention are essentially "symmetric" as that term is known in the art. Whereas one
24

If A XOR B, C, D, E = F, then F XOR B, C, D, E = A

For example, 57 XOR 254, 16, 92, 133 = 14, so 14 XOR 254, 16, 92, 133 = 57,
which is better understood by the binary numbers depicted below:

57:	00111001	14:	00001110
XOR 254:	<u>11111110</u>	XOR 254:	<u>11111110</u>
199:	11000111	240:	11110000
XOR 16:	<u>00010000</u>	XOR 16:	<u>00010000</u>
215:	11010111	224:	11100000
XOR 92:	<u>01011100</u>	XOR 92:	<u>01011100</u>
139:	10001011	188:	10111100
XOR 133:	<u>10000101</u>	XOR 133:	<u>10000101</u>
14:	00001110	57:	00111001

The XOR process is also commutative, which means that the same result is
obtained regardless of the order of operation, hence,

If A XOR B, C = F, then A XOR C, B = F

This property of XOR is not necessarily a desirable property for the purposes of
encryption and decryption because it makes the ciphertext easier to decrypt. Thus, it may
also be beneficial to apply an additional mathematical operator in combination with XOR
that will make the process noncommutative. For example, adding or subtracting 1 or

1 changing or all of the bits to their complement (i.e., 0 for 1 and vice versa) would render
2 the process noncommutative. Thus, the XOR process may advantageously be modified
3 or combined with another mathematical process so that it is not commutative.

4 Exemplary methods for implementing the encryption and decryption systems
5 according to the present invention (including the encryption and decryption systems 90
6 and 92 depicted in Figures 2A and 2B, respectively, and described herein) will be
7 discussed more fully below.

8
9 **C. Communication System Between Encrypting and Decrypting Parties.**

10 The inventive methods and systems for encrypting and then decrypting electronic
11 files according to the invention may be implemented in any desired manner, and are well
12 suited for the case where a single encrypting party wishes to send a number of different
13 encrypted files to various receiving parties. The communication interface between the
14 sending and receiving parties may comprise any desired communication system known in
15 the art or which may be developed in the future. Examples include dedicated phone
16 lines, the Internet, ordinary mail and the like.

17 Figure 3 illustrates an exemplary communication system 150 between a sending
18 party 152 (typically the encrypting party) and a receiving party 154 (typically the
19 decrypting party). One exemplary communication channel comprises a less secure
20 communication channel 156 that involves, or passes through, the Internet infrastructure
21 158. A secure socket layer (e.g., via HTTPS) can be used to more securely communicate
22 between the sending party 152 and the receiving party 154. Another example is a
23 dedicated phone line 160 or secure digital channel. Another is a courier service 162, such
24 as ordinary mail, used to transmit hard or tangible copies of appropriate storage media

1 containing digital information. The dedicated phone line 160 generally provides more
2 security than a communication channel 156 involving the Internet 158. Likewise, a
3 courier service 162 generally provides greater security compared to a dedicated phone
4 line 160. The preferred communication channel will depend on the information being
5 shared and the security that is desired.

6 The encrypted files and their respective "public keys" may be sent over any
7 desired communications channel known in the art, including both secure and nonsecure
8 channels. One presently preferred communication system is over the Internet 158.
9 Because the security of the encryption and decryption systems of the invention are
10 dependent on maintaining the secrecy of the private key rather than the public key, and
11 because the encrypted file cannot be decrypted without the private key (at least not
12 without tremendous effort), the new file type comprising an encrypted file 118 and
13 corresponding public key 112 (Figures 2A and 2B) may be sent over a nonsecure
14 channel. Because the Internet is presently the least expensive nonsecure channel over
15 which to send electronic data, it presently constitutes the preferred system for
16 transmitting an encrypted file and its public key to the requesting third party.
17 Nevertheless, the encrypted file may be sent by other means, such as over a secure
18 channel 160 or by courier service 162.

19 On the other hand, the system for communicating the private key to the
20 decrypting party must generally be secure so as to prevent interception by unauthorized
21 third parties. In the case where a single private key is used to encrypt and then decrypt a
22 plurality of different electronic files, the private key may be sent to each of the decrypting
23 parties using a secure channel, such as through ordinary mail 162 via a CD-ROM, floppy
24 disk or other appropriate storage medium. An advantage of this system is that it allows a

FILED 02-04-2009

1 repeat customer to continually decrypt each new encrypted file using the same private
2 key. A weakness of this approach is the ability of a rogue customer to simply copy the
3 private key and/or share it with unauthorized third parties.

4 Another exemplary system for communicating the private key is a dedicated
5 phone line 160 between the encrypting and decrypting parties that may be accessed
6 through a password-protected login procedure. A weakness of this approach is the ability
7 of an eavesdropper to intercept the private key using a wiretap or other surveillance
8 method. A private key that is used to encrypt and decrypt many files may be prone to
9 being intercepted and used to decrypt files that are subsequently sent by the same
10 encrypting party. Nevertheless, so long as the secrecy of the private key is carefully
11 maintained, encryption and decryption systems using a single private key to encrypt
12 many files can be very secure, particularly if the overall key (public and private
13 components) is difficult to decipher. One way to increase the difficulty of intercepting
14 the private key is to use an additional encryption algorithm and associated key to encrypt
15 the private key, thereby creating additional hurdles for a motivated hacker to overcome.

16 In another embodiment of the invention, the private key is regenerated
17 periodically so that a hacker would have to intercept each new private key as it is
18 generated in order to decipher the encrypted files. In the most secure system, a new
19 private key is generated for each new file that is encrypted, thus requiring a hacker to
20 intercept and/or decipher the private key each and every time a new file is encrypted and
21 sent from the encrypting party to the authorized decrypting party. In theory, this
22 approach at least partially resembles a "one-time pad," which is theoretically the most
23 secure encryption system possible.
24

1 In a true one-time pad system, the key is at least the same length as the message
2 being encrypted, so that the key sequence is never repeated. In addition, the key is
3 available only to the encrypting and decrypting parties. As stated above, the huge
4 variability inherent in how the private and public keys operate together make the chance
5 of repetition of the overall cipher during encryption very rare. This makes it very
6 difficult and time-consuming for a hacker to decipher the private key. Moreover, because
7 a deciphered private key can be used to decrypt only a single encrypted document where
8 a new private key is generated for each encrypted file, there may be very little incentive
9 for a hacker to expend the time and resources necessary to decipher any particular private
10 key. The primary weakness in this encryption system would be in the ability of a hacker
11 to intercept the private key during transmission from the encrypting party to the
12 decrypting party. Once again, a dedicated phone line requiring a password-protected
13 login procedure would appear to provide adequate protection from interception so long as
14 the dedicated phone line was not bugged. Of course, additional layers of protection, such
15 as encrypting the private key and/or public key using a second secure key known only to
16 the encrypting and decrypting parties, may make it costlier in terms of time and resources
17 to decipher the encrypted keys and associated electronic file than the value of the
18 information contained within the encrypted file. This alone may deter most, if not all,
19 hackers from even caring to decipher the private key and associate encrypted file.

20
21 **D. Controlled Output System for Decrypted Files.**

22 Notwithstanding each of the foregoing systems for securely encrypting and then
23 sending an encrypted file to an authorized third party while carefully maintaining the
24 security of the private key(s), care must be taken to prevent unauthorized access to the

1 decrypted file. Accordingly, a preferred system for decrypting an encrypted file will also
2 include safeguards that will prevent (or at least make it substantially difficult for) the
3 decrypting party to copy, alter or send the decrypted plaintext file. Because the electronic
4 file is encrypted, it will be virtually impossible to view anything other than an apparently
5 corrupt file using commercially available software, such as standard word processing
6 programs, graphic viewing programs, or spreadsheet programs.

7 In a preferred embodiment according to the invention, the software that is
8 necessary to decrypt the file, including the decryption module 106', will preferably be
9 integrated together with an output or viewing system that does not allow the viewing
10 party to copy, alter or send the decrypted plaintext file. Figure 4 illustrates an integrated
11 decryption/output system 94 that includes the decryption system 92 and an output system
12 96. The decryption system 92 provides the decrypted plaintext, or original file 100, to the
13 output system 96, which further includes a front end module 97 for decoding, organizing
14 or otherwise making logical sense of the original plaintext file 100, which sends
15 displayable data 98 to an output apparatus 99 for display or other method for outputting
16 the displayable data 98.

17 In a preferred embodiment, the front end module 97 may be configured so as to
18 severely limit the ability of a decrypting party to copy, alter or send the original plaintext
19 file 100. The software may be limited, for example, to simply supplying an electronic
20 signal for display to a monitor or printer. To be sure, a sophisticated hacker working for
21 the decrypting party might be able to find a way to overcome the barriers erected to
22 prevent copying, altering or sending the decrypted file. Of course, having a mole or spy
23 in any organization would defeat virtually any security system. In most cases, the people
24 typically assigned the task of decrypting an encrypted file in, e.g., an insurance company,

1 hospital, law firm or government bureaucracy, should be carefully screened and trusted
2 individuals.

3 In the case where the encrypted file comprises part of a new file type, such as new
4 file type 116 (Figures 2A and 2B), that includes the public key 112 appended to the front,
5 back, middle or other location within the encrypted file 118, the decryption/output
6 software will advantageously know where to find the public key 112 from among the rest
7 of the electronic data corresponding to the actual encrypted file 118. In a present
8 embodiment, the public key 112 is appended to the front of the file, and the new file type
9 116 is identified by a unique identifying suffix appended to the file name (*e.g.*, Corel
10 Word Perfect® documents are appended with the suffix “.wpd” while Microsoft Word®
11 documents are appended with the suffix “.doc”).

12 Appending the new file type with the unique appendix serves at least two
13 purposes. One is that conventional software programs will not recognize this unique file
14 type, thus providing at least a first layer of confusion to a potential copier. Another is
15 that the software required to decrypt and output this unique file type will work only for
16 files having the unique suffix appended thereto, thus making the software of no value to
17 the decrypting party for tasks other than decrypting and displaying the unique file types
18 bearing the proper suffix. This will also tend to prevent unauthorized copying of the
19 decryption/output software. In any event, because the decryption/output software is
20 programmed so as to first identify the public key and then decrypt the remaining
21 electronic file using the associated private key, it is incapable of displaying anything
22 other than corrupt information unless the file being acted upon has been encrypted
23 according to the systems and methods disclosed herein.

One way to determine whether a file has been altered would be for the viewer to validate the file in question against the copy stored or owned by the encrypting party, typically through an SSL connection. For example, additional numeric information specific to a particular file (*i.e.* a digital signature) could be stored together with, or as part of, the private key. If the signature information of the file in question does not match the signature information for that file in the possession of the encrypting party, then the file in question has been altered from the original version. Such a scenario would require at least the signature portion of the private key to be unique for each encrypted file.

In the case where the original file is in graphic form, such as a TIFF file, the output program, in addition to decrypting the encrypted file portion of the new file type, will advantageously be capable of decoding and displaying and/or printing the TIFF or other graphic file (*e.g.*, GIF, JPEG, or BMP). However, it will preferably not provide the decrypting party with the ability to copy, alter or send the decrypted plaintext file. Though obviously restricted in terms of flexibility and features, the limited number of features of the preferred output program make it less cluttered, more intuitive, and easier to use.

III. METHODS FOR ENCRYPTING AND DECRYPTING FILES.

Exemplary methods for encrypting and decrypting electronic files according to the invention should be readily apparent from reading the descriptions of the systems set forth above. Such methods generally include serially encrypting blocks of electronic data (*e.g.*, binary data) using the public and private keys, saving the encrypted blocks, preferably together with the public key, sending the encrypted file to an authorized decrypting party, serially decrypting blocks of the encrypted file using the public and

1 private keys, and outputting the original file. They also include specific algorithms for
2 navigating through, or integrating, the public and private keys during each encryption or
3 decryption sequence per block of electronic data.

4
5 **A. Generation of Encryption Keys.**

6 Before a file can be encrypted, public and private keys must be provided. The
7 public and private keys each contain serially indexed integer values within predetermined
8 ranges. The number and range of integer values, as well as their randomness, will depend
9 on the level of security that is desired for encryption and decryption of a given file. An
10 exemplary process for generating a key includes the steps of (1) determining how many
11 integer values to include, (2) assigning a sufficient number of indexes to accommodate
12 each integer value, and (3) serially filling each index with a randomly or pseudo-
13 randomly generated integer values within the specified range.

14 The integer values may be generated using any random number generator known
15 in the art, with the caveat that some random number generators are less random than
16 others. Less sophisticated "random number" generators may actually create patterns that
17 are discernable to hackers. The more "random" the string of random numbers is, the
18 more secure the key will be. A common random number generator uses the clock to
19 generate a seed value to begin the random number generation process. Although
20 randomly selected integer values provide for a more secure cipher, it is certainly within
21 the scope of the invention to include integer values that are not totally random.

1 **B. Encrypting and Decrypting Electronic Files.**

2 Figure 5A illustrates an exemplary encryption process 170 that generally outlines
3 general steps for encrypting files within the scope of the present invention. In a first step,
4 an original file is provided together with corresponding public and private keys. A block
5 of cleartext is selected for encryption. A first random number is selected from the private
6 key and then input into the public key in a manner so as to obtain one or more random
7 numbers. The private key supplies an index number for input into the public key to
8 obtain the one or more random numbers. The one or more random numbers from the
9 public key are then used to encrypt the block of cleartext by means of an XOR process.
10 This process is repeated until the entire plaintext file has been encrypted. The encrypted
11 blocks are stored together with the public key to form a unique file type, preferably
12 including a unique suffix identifiable by special decryption software used to later decrypt
13 the encrypted ciphertext.

14 In a preferred embodiment, a unique public key will be generated and provided
15 with each new original plaintext file to be encrypted. The private key may be used to
16 encrypt either one or a plurality of files. In general, generating a new private key for
17 each new plaintext file to be encrypted yields a more secure encryption process.

18 Figure 5B illustrates an exemplary process for decrypting the ciphertext generated
19 by the process illustrated in Figure 5A, and is essentially the same, or mirror image of the
20 encryption process. In a first step, an encrypted file is provided together with
21 corresponding public and private keys. A block of ciphertext is selected for decryption.
22 A first random number is selected from the private key and then input into the public key
23 in a manner so as to obtain one or more random numbers. The private key supplies an
24 index number for input into the public key to obtain the one or more random numbers. In

1 a preferred embodiment, the random numbers selected from the private and public keys
2 for any given block of ciphertext will be the same as those used to encrypt the block of
3 cleartext corresponding to that block of ciphertext. The one or more random numbers
4 from the public key are then used to decrypt the block of ciphertext by an XOR process.
5 Because the XOR process is reversible, performing an XOR process on the ciphertext
6 using the same random numbers used to create the ciphertext restores the plaintext block.
7 This process is repeated until the entire ciphertext file has been decrypted and the original
8 plaintext file has been restored.

9 The algorithm used for encryption and decryption includes as a subcomponent a
10 mathematical relationship that allows the private and public keys to meaningfully interact
11 with each other in the same way during encryption and decryption. Because the
12 encryption and decryption systems according to the invention are symmetrical, the same
13 algorithm used to encrypt the plaintext file will also preferably be used to decrypt the
14 encrypted file, or ciphertext. Accordingly, the algorithm used to integrate the private and
15 public keys together will be known to both the encrypting and decrypting parties, and
16 preferably to no one else.

17 Figure 6 illustrates an exemplary algorithm or method 123 used to integrate the
18 private and public keys together during encryption and decryption. The first step
19 involves selecting a random number value from a private key 124 that includes an index
20 125 and a list 127 of corresponding random numbers. According to a predetermined
21 algorithm, to be discussed below, an index position 126 (e.g., 1043) is input into the
22 private key 124 in order to obtain a corresponding random value 128 (e.g., 983). The
23 random number 128 is then input into a corresponding public key 130 that includes an
24 index 131 and a list 133 of corresponding random numbers in order to obtain one or more

1 random numbers. Although it is within the scope of the invention to select only one
2 random number from the public table 130 for encrypting each block of electronic data, it
3 will be preferable to select one or more random values in order to introduce greater
4 randomness into the XOR process and the resulting encrypted block.

5 As an example of how to determine how many random numbers to select from the
6 public key 130, the random number 128 selected from the private key may be used to
7 determine how many random numbers 132 to select from the public key 130. As
8 depicted in Figure 6, the random number 128 (*e.g.*, 983) is divided by a predetermined
9 divisor (*e.g.*, 20) and the resulting remainder 129 (*e.g.*, 3) is used to determine how many
10 total random values to select from the public key 130. Although the random numbers
11 may be selected in any desired manner or sequence from the public key 130, in an
12 exemplary method, the random number 128 selected from the private key (*e.g.*, 983) is
13 the beginning index position of the public key 130. Additional random numbers are
14 selected serially by moving to the next successive index position until the predetermined
15 number of random numbers corresponding to the remainder 129 (*e.g.*, 3) having been
16 selected from the public key 130. Hence, according to the example illustrated in Figure
17 6, the three random numbers 132a, 132b, and 132c selected from the public table 130
18 correspond to index positions 983–985, respectively.

19 The three random numbers 132a–c (*e.g.*, 3, 255 and 98) selected from the public
20 table 130 are then used to encrypt a block 136 (*e.g.*, 121) of the cleartext 134 using an
21 XOR process 138. For example, $121 \text{ XOR } 3 = 122$, which is a first intermediate
22 encrypted block 140a; $122 \text{ XOR } 255 = 133$, which is a second intermediate encrypted
23 block 140b; and $133 \text{ XOR } 98 = 231$, which is the final encrypted block 140c. The final
24 encrypted block 140c is stored together with other encrypted blocks as part of an

1 encrypted file 142. Upon encrypting a block of the original file, process 123 is then
2 repeated for the next block.

3 The first step of repeating the process 123 for the next block involves updating the
4 index of the private key. Although this may be performed using any desired
5 mathematical relationship, in an exemplary method of the invention, an updating step 144
6 is carried out by adding the numeric value of the encrypted block 140c to the original
7 index position 126 (*e.g.*, 1043) to yield a new index position 126' (*e.g.*, $1043 + 231 =$
8 1274). The new index position 126' is then input into the private key 124 during the next
9 iteration of the encryption process 123. As will be discussed more fully below, when a
10 newly determined index position exceeds the number of index positions in the private
11 key, the index position is reset to the starting position (*e.g.*, 0), and a preselected
12 increment (*e.g.*, 1) is added to prevent repetition and introduce additional randomness.

13 In the case where the data stream is to be encrypted one byte at a time, the random
14 numbers selected from the public key will be in a range inclusive of 1 to 255. The
15 number "0" is typically not used because XORing with the number "0" does not change
16 the original value.

C. Updating the Private Key.

An exemplary process for updating the index position for the private key during each iteration of the encryption or decryption processes according to the invention is illustrated in Figures 7A and 7B. When encrypting or decrypting the first block in an electronic file, the random number corresponding to index position 0 is selected and input into the public table, as described elsewhere, to obtain one or more random numbers used to encrypt or decrypt the first block. In order to prevent a string of repetitive data from having the same repetitive pattern in the encrypted result, it may be advantageous to update the index position in a more random manner than simply adding 1 or some other pre-selected number to the index position.

As shown in Figure 7A, a presently preferred way to randomly update the index 192 of the private key 190 is to add the encrypted block value to the previous index position. Hence, if encrypting the first block of cleartext yields 57 as the encrypted block, 57 is then added to 0 such that 57 is the next index position used to select a random number from the private key 190 for the next iteration of the encryption process. Each of the successive encrypted block values (*e.g.*, 230, 165, 19, 98, etc.) is used to incrementally update the index position (*e.g.*, 287, 452, 471, 569, . . . 2022) for each successive iteration of the encryption process.

At some point, when the next calculated index position (*e.g.*, 2022 + 71) is greater than the highest index position (*e.g.*, 2047), the next actual index position is selected by returning to the beginning index position, plus some predetermined increment, *e.g.*, 1, as illustrated in Figure 7B. Thus, when the predetermined increment is 1, the position is reset to the beginning index position (*i.e.*, 0) but offset by the number of times the position has gone past the ending index position of the private key. When the offset

1 exceeds the ending index position of the private key, it is reset to 0 or some other
2 number. If repetition becomes a problem, the key sizes can be increased to delay the
3 appearance of repetitive patterns in the encrypted result.

4 In order to restore the plaintext during encryption, the private key index position
5 is updated in the same manner as during encryption so that the same random numbers
6 used to encrypt a block of data is used to decrypt the corresponding block of ciphertext.
7 In this manner, the original cleartext is restored in a symmetric encryption/decryption
8 process.

9
10 **D. Outputting the Decrypted File.**

11 After an encrypted file has been decrypted so as to restore the original plaintext
12 file, the contents may be displayed, saved, manipulated, duplicated, altered or shared
13 using any appropriate software known in the art for the particular file type in question.
14 Nevertheless, in order to preserve the confidentiality and integrity of the original file, it
15 may be preferable to limit the ability of the decrypting party to save, share or alter the
16 data contained therein.

17 Accordingly, in a preferred method for outputting the decrypted file the
18 decrypting will be limited to merely viewing and/or printing out a hard copy of the
19 decrypted file. This may be accomplished by providing the decrypting party with special
20 software, as described herein, that integrates the decryption and outputting processes so
21 as to provide the decrypting party with only limited access to the information contained
22 in the decrypted file. The software will first perform the decryption process described
23 herein using the private and public keys together with the decryption algorithm, followed
24 by a controlled outputting process that preferably provides no options to the end user that